Information Security Officer Meeting

November 10, 2009

Meeting Agenda

- Short Subjects:
  - Cyber Security Awareness Month 2009 Retrospective
  - Legislation Update
  - The Information Security Profession is Changing
  - SIMM Form and Leader List Updates
- California Information Security Strategic Plan
- Incident Management
- New Information Security Policy
  - Phase I – Vetting
  - Phase II – Preparing to vet

Cyber Security Awareness Month 2009 A California Retrospective

Office of Information Security
OCIO

1. September 30, 2009 –CISO Lecture Series
2. October 1, 2009 – Governor Schwarzenegger signed National Cyber Security Awareness month proclamation
3. October 1, 2009 –Cyber Security Awareness statement on all state employee pay warrants
4. October 4, 2009 – Four weekly security awareness bulletins.
5. October 8, 2009 - Emergency Awareness Fair
6. October 14, 2009 –West Coast Kickoff Conference for National Cyber Security Awareness Month titled *"Cyber Security West 2009: Our Shared Responsibility"*
7. October 15, 2009 – Participated in the CISO Executive Summit in San Francisco
8. October 21/22 - California State Security Awareness Fair

Cyber Security Awareness Month 2009
A National Retrospective

1. The first time all 50 states participated in Cyber Security Month by issuing an executive proclamation
2. The first time the President has issued a proclamation
3. Whitehouse BLOG and presidential video
4. The first time the United States House of Representatives issued a proclamation
5. The first time the U. S. Senate issued a proclamation
6. National Webcast Initiative hosted by MS-ISAC
7. DHS Secretary Napolitano Webinar on Cyber Security Month

Cyber Security Awareness Month 2010 Planning

- More handouts?
- Radio and TV spots?
- National Poster Contest?
- Is there more we can do as a community?
- Your ideas?

Legislation Update

Office of Information Security
OCIO

LEGISLATIVE WATCH UPDATE

Introduced: California (Either Legislative House introduced a bill)

AB 5 Civil Discovery: Electronic Discovery Act Status: Chaptered

This bill would make changes to the Civil Discovery Act in order to take account of the growing volume of information stored in electronic form. Existing law permits a party to obtain paper documents and other "tangible" things from the opposing party. However, the increasing use of electronically and digitally stored documents and information has many implications for the discovery process, affecting not only the volume but the form of discoverable material. This bill expressly authorizes the discovery of electronically stored information and amends procedures in existing law so as to better address issues unique to the format of such information. Many of the bill's specific provisions are drawn from recently enacted federal rules and from recommendations of the National Conference of Commissioners on Uniform State Laws. The bill is co-sponsored by the Judicial Council, the Civil Defense Counsel, and the Consumer Attorneys of California. Except for a few non-substantive technical changes and the addition of an urgency clause, the bill is identical to last year's AB 926 by the same author. That bill passed out of this Committee on consent and passed out of all other Committees and off the floors of both houses without a single dissenting vote. AB 926 was vetoed, but as one of the many bills that the Governor vetoed because of his stated concerns about not having sufficient time to review much of that year's legislation due to the budget crisis.

AB 22 Penal Code, relating to computer hacking Status: Chaptered

As originally introduced this bill would increase the maximum fines for those convicted of feloniously tampering, interfering, damaging, and obtaining unauthorized access to computer data and computer systems from the current maximum of $10, 000 to a maximum of $50,000. This bill was recently amended to increase the fine for the felony conviction to an amount not exceeding $12,000.

AB 32 Public officials: personal information Status: Chaptered

This bill would require the removal of personal information of specified officials from the Internet, and permits employers or professional organizations to assert the rights of the official in removing the personal information from the Internet. With regard to a violation of this prohibition, existing law requires a jury or court that finds a violation has occurred to award damages to that official in an amount up to a maximum of 3 times the actual damages but not less than $4,000. This bill proposes to instead require a jury or court to award damages in that amount to an official whose home address or telephone number is solicited, sold, or traded in violation of any of those prohibitions.

AB 130 Vital records: marriage records Status: Chaptered (10-11-09)

By changing the definition of the crime of perjury, and by imposing new duties on local officials, this bill would create a state-mandated local program.

AB 255 Internet security: virtual globe technology Status: Active

Existing law requires the operator of a commercial Internet Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Internet Web site or online service to post its privacy policy on its Internet Web site or make that policy available, as specified. This bill would prohibit an operator, as defined, of a commercial Internet Web site or online service that makes a virtual globe browser available to members of the public from providing aerial or satellite photographs or imagery of places in this state that have been identified on the Internet Web site by the operator as

Information Security Profession

Office of Information Security
OCIO

- Becoming more “cyber” but it’s still all about “risk”
- Full-time focus
- Can’t leave it at the office
- National impact
- More than just financial harm

SIMM Form and Leader List Updates

SIMM Form Changes:

- Name Change from OISPP to OIS
- Other minor clarification changes
- SIMM70A (Agency Designation Letter) and
- SIMM70C (Agency Risk Management and Privacy Program Compliance Certification)
- Forms due January 31, 2010

Leader List Updates for:

- Information Security Officers
- Privacy Officers and
- DR Coordinators
- All available on website by 11/30/09

California Information Security Strategic Plan

Office of Information Security
OCIO

California Information Security Strategic Plan

October

2009

Cybersecurity and Privacy Concepts, Strategies & Goals
Volume 4

Arnold Schwarzenegge
Governo

Teri Taka
Chief Information Officer, Office of the CI

Mark Weatherfor
Chief Information Security Officer, Office of Information Securit

OCIO 2009 Information Technology Strategic Plan

Six Strategic Concepts

- IT as reliable as electricity
- Fulfilling technology's potential to transform lives
- Self-governance in the digital age
- Information as an asset
- Economic and sustainable
- Facilitating collaboration that breeds better solutions

Overview of US-CERT & MS-ISAC Security Notifications

Office of Information Security
OCIO

- Who are US-CERT and MS-ISAC
- Types of Security Notifications

Housekeeping

UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO)
Can I distribute or share this information with other people?

Per the U//FOUO warning, this document may only be shared with personnel who have a valid "need to know." With the case of the information about to be shared that is defined as a person or group that has a direct role in responding to the types of security incidents discussed herein.

Who are they?

Office of Information Security
OCIO

Who is US-CERT?

- United States Computer Emergency Readiness Team
- Operational arm of the National Cyber Security Division at the Department of Homeland Security
- A public-private partnership

http://www.us-cert.gov/

Who is MS-ISAC?

- Multi-State Information Sharing and Analysis Center
- A collaborative organization with participation from all 50 States, the District of Columbia, local governments, and U.S. Territories
- A central resource for gathering information on cyber threats to critical infrastructure from the states

http://www.msisac.org/

US-CERT & MS-ISAC Security Notifications

Office of Information Security
OCIO

XSS Vulnerability Detection

- Host reported to MS-ISAC as having one or more XSS vulnerability
- Host may have other application-level vulnerabilities
- Host could be used by attacker in attempt to attack other hosts

Web Defacement Detection

- Host appears to have a public-facing web defacement
- Notification is made when website appears to still be defaced

DarkNet General Traffic Detection

- Host has sent traffic captured by the EINSTIEN program
- Host is possibly compromised with some kind of malware attempting to propagate on the public Internet

US-CERT & MS-ISAC Security Notifications

Office of Information Security
OCIO

CySearch

- MS-ISAC uses its custom tool to search the Internet for:
  1. Inappropriate terms (e.g., porn, Viagra, free Rolex watches). Attackers inject these terms along with links to web pages to boost ranking in various search engines
  2. Indicators of malicious activity on government websites (e.g., malicious domain names, IP addresses, JavaScripts, hidden iframes)

Information Security Policy Phase I - Vetting

Information Security Policy
Phase II – Preparing to Vet

5315	Organization
5320.1	Information Asset Oversight
5320.2	Information Asset Trustees
5320.3	Users of Information Assets
5320-S1	Information Asset Classification Standard
5320-S2	Information Asset Handling Standard
5330.1	Facility Leader Responsibilities
5330.2	Information Asset Trustee Responsibilities
5340.1	Access Management Standard
5340.2	User Responsibilities
5340-S1	User Access Management Standard
5340-S2	Password Management Standard

Information Security Policy
Phase II – Preparing to Vet

5355	Disaster Recovery
5355-S1	Disaster Recovery Standard
5360-P1	Annual Compliance Reporting Procedure
5365.1	Agency Heads Responsible
5365.2	Agency Privacy Statement and Notices
5365.3	Limiting Collection
5365.4	Limiting Use and Disclosure
5365.5	Individual Access to Personal Information
5365.6	Information Integrity
5365.7	Data Retention and Destruction
5365.8	Security Safeguards
5365-S1	Privacy Statement and Notices Standard
5365-S2	Individual Access Standard

Office of Information Security
OCIO

Questions